October 1999

Back circulant Latin squares and the influence of a set

L. F. Fitina
University of Wollongong

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

G. R. Chaudhry
University of Wollongong

Back circulant Latin squares and the influence of a set

Abstract

We define the notions of nest and influence of a subset of a critical set of a back circulant latin square, and study their properties. We also show that a secret sharing scheme based on a critical set of a latin square is both compartmentalised, and hierachical.

Disciplines

Physical Sciences and Mathematics

Publication Details

This article was originally published as Fitina, LF, Seberry, J and Chaudhry, GR, Back circulant Latin squares and the influence of a set, Australasian Journal of Combinatorics, 20, 1999, 163-180.

Back circulant Latin squares and the influence of a set

L F Fitina, Jennifer Seberry and Ghulam R Chaudhry
Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
NSW 2522
Australia

October 1, 1999

Abstract

We define the notions of nest and influence of a subset of a critical set of a back circulant latin square, and study their properties. We also show that a secret sharing scheme based on a critical set of a latin square is both compartmentalised, and hierachical.

1 Introduction

A *latin square* L of order n is a $n \times n$ array with entries chosen from a set N of size n, such that each element of N occurs precisely once in each row and column. Thus L may be thought of as a set of triples $(i, j; k)$, where $k = i + j$ is the entry in cell (i, j). L is said to be *backcirculant* if $N = \{0, 1, \ldots, n-1\}$, and $k = i + j \bmod n \ \forall \ i, j \ \in \ N$. Let L be a back circulant latin square of order n given by $L = \{(i, j; i + j)\}$ with addition reduced modulo n. If A is any subset of L, we call the set of cells in A the *shape* of A. A is called a *critical set* of L, if (i) L is the only latin square of order n which has element k in position (i, j) for each $(i, j; k) \in A$, and (ii) no proper subset of A satisfies (i). A set $A \subseteq L$ having property (i) is called *uniquely completable* and each element in it is also said to be uniquely completable. Every subset A of L is said to be *uniquely filled* or *fillable*. Let $\frac{n-3}{2} \leq r \leq n-2$. Donovan and Cooper [3] proved that the set

$$C = \{(i, j; i + j) : i = 0, \ldots, r \text{ and } j = 0, \ldots, r - i\}$$

$$\cup$$

$$\{(i, j; i + j) : i = r + 2, \ldots, n - 1 \text{ and } j = r + 1 - i, \ldots n - 1\}$$

with $\frac{n-3}{2} \leq r \leq n-2$, is a critical set in L. Note that C is the union of two triangles, which we call the *upper triangle* and the *lower triangle*. If $B \subseteq C$ is a subset of the critical set define the *nest* $\mathcal{N}(B)$ of B to be the union of $C \setminus B$ and the set that can be uniquely filled when B is deleted from C. Define the *influence-set* of B, denoted $\mathcal{I}(B)$, to be the shape of the set $\{L \setminus \cup\{\mathcal{N}(b) : b \in B\}$. The number $|\mathcal{I}(B)|$ is called the *influence* of B, and denoted by $\theta(B)$. The set $\mathcal{I}(C)$ is called the *strong box* of L. A set $B \subset C$ is said to have *perfect influence* if $B \cup \mathcal{N}(B) = C$. A collection $\mathcal{K}$ of partial latin squares I is called a *latin collection* if the entries in the cells of each row (and column) of each $I \in \mathcal{K}$ are the same as those in the corresponding row (and column) of every other partial square in $\mathcal{K}$, and if the intersection of all the partial latin squares, regarded as sets of triples, is empty. A *latin interchange pair* is a latin collection of size 2. (See also [3] for an equivalent definition.) Elements of a latin interchange pair are called latin interchanges, and each is called the disjoint mate of the other. If A is a set and x is

any element, we will often write xA for the set $\{x\} \cup A$. Let $x, y \in C$. We write $x \rightsquigarrow y$ (x *leads to* y) if there exist sets $A, B \subseteq C$ with non-perfect influences, such that the following conditions hold:

LT1 $x \notin A, x \notin B, y \notin A, y \in B$

LT2 xA has perfect influence

LT3 $A \cup B$ has perfect influence

LT4 $A \cup B'$ does not have perfect influence, for any proper subset B' of B.

We say x is *more influential than* y, and write $x \longrightarrow y$ if

MI1 There is a finite sequence of the form: $x \rightsquigarrow z_1 \rightsquigarrow z_2 \rightsquigarrow \ldots z_m \rightsquigarrow y$
and

MI2 There is no finite sequence of the above form from y to x.

If $x, y \in C$, we define the relation $x \sim y \Longleftrightarrow \theta(x) = \theta(y)$. Clearly $\sim$ is an equivalence relation. For any $x \in C$, define $[x]$ to be the equivalence class of x. Define the *index of* C to be the total number of influence classes.

We give now an example to illustrate some of these definitions:

Example 1 Consider the critical set for the 9×9 back circulant latin square:

0	1	2	3					
1	2	3						
2	3							
3								
								4
							4	5
						4	5	6
					4	5	6	7

Let $\alpha = (0, 0; 0)$, $\beta = (8, 8; 7)$, $\beta_1 = (8, 5; 4)$, $\beta_{col} = (7, 8; 6)$. The nests and influence-sets of these entries are as follows:

	1	2	3					
1	2	3						
2	3							1
3							1	2
						1	2	3
					1	2	3	4
				1	2	3	4	5
			1	2	3	4	5	6
		1	2	3	4	5	6	7

Nest of α

*				*	*	*	*	*
			*	*	*	*	*	*
		*	*	*	*	*	*	
	*	*	*	*	*	*		
*	*	*	*	*	*			
*	*	*	*	*				
*	*	*	*					
*	*	*						
*	*							

Influence-set of α

0	1	2	3	4	5	6		
1	2	3	4	5	6			
2	3	4	5	6				
3	4	5	6					
4	5	6						
5	6							4
6							4	5
						4	5	6
					4	5	6	

Nest of β

							*	*
						*	*	*
					*	*	*	*
				*	*	*	*	*
			*	*	*	*	*	*
		*	*	*	*	*	*	
	*	*	*	*	*	*		
*	*	*	*	*	*			
*	*	*	*	*				*

Influence-set of β

0	1	2	3			6	7	8
1	2	3				7	8	0
2	3					8	0	1
3						0	1	2
						1	2	3
						2	3	4
						3	4	5
						4	5	6
						5	6	7

Nest of β_1

				*	*			
			*	*	*			
		*	*	*	*			
	*	*	*	*	*			
*	*	*	*	*	*			
*	*	*	*	*	*			
*	*	*	*	*	*			
*	*	*	*	*	*			
*	*	*	*	*	*			

Influence-set of β_1

0	1	2	3	4	5			
1	2	3	4	5				
2	3	4	5					
3	4	5						
4	5							
5								4
							4	5
						4	5	
8	0	1	2	3	4	5	6	7

Nest of β_{col}

						*	*	*
					*	*	*	*
				*	*	*	*	*
			*	*	*	*	*	*
		*	*	*	*	*	*	*
	*	*	*	*	*	*	*	
*	*	*	*	*	*	*		
*	*	*	*	*	*			*

Influence-set of β_{col}

It can be seen on inspection, that the sets $\{\alpha, \beta\}$ and $\{\beta, \beta_1, \beta_{col}\}$ have perfect influence. Let $A = \{\beta\}$, and $B = \{\beta_1, \beta_{col}\}$. Clearly, $\alpha \notin A$, $\alpha \notin B$, $\beta_1 \notin A$ and $\beta_1 \in B$. $\alpha A = \{\alpha, \beta\}$ has perfect influence. Similarly, $A \cup B = \{\beta, \beta_1, \beta_{col}\}$ has perfect influence. On the other hand, it can be easily verified that neither $\beta_1 A = \{\beta, \beta_1\}$, nor $\beta_{col} A = \{\beta, \beta_{col}\}$ has perfect influence. Thus by definition, $\alpha \rightsquigarrow \beta_1$. Note also that $\beta_1 \rightsquigarrow \alpha$. Similarly $\alpha \rightsquigarrow \beta_{col}$, but it is not true that $\beta_{col} \rightsquigarrow \alpha$, therefore $\alpha \longrightarrow \beta_{col}$, or α is more influential than β_{col}.

Conjecture 1 *For any $x, y \in C$, $x \rightsquigarrow y \Longrightarrow \theta(x) \leq \theta(y)$.*

Conjecture 2 *Let L be a back circulant Latin square of odd order n and critical set C, with $r = \frac{n-3}{2}$. Then the index of C is r.*

In this paper we study the influence of sets that are subsets of the critical sets C discussed above.

2 Some general results

In this section we calculate the nests and the sizes of these nests for different entries of the critical set. These will be useful in the later sections where we calculate the influence of certain sets.

In the following lemmas we show that some rows, columns and diagonals can be completed after the deletion of an element.

Lemma 1 *Suppose $(i,j;k)$ is deleted from the lower triangle of the critical set C. Then every column $\lambda, j < \lambda \leq n-1$ can be uniquely filled, and every row $\gamma, i < \gamma \leq n-1$ can similarly be uniquely filled.*

Similarly if $(i,j;k)$ was in the upper triangle then columns $\lambda, 0 \leq \lambda < j$ can be filled, as can rows $\gamma, 0 \leq \gamma < i$.

Proof. Neither row γ nor column λ depend on the information contained in row i or j, and thus can be filled uniquely.

□

We now show that some diagonals can be filled.

Lemma 2 *Let the critical set C be*

$$C = \{(i,j;i+j) : i = 0,\ldots,r \text{ and } j = 0,\ldots,r-i\}$$

$$\cup \ \{(i,j;i+j) : i = r+2,\ldots,n-1 \text{ and } j = r+1-i,\ldots,n-1\},$$

where $(n-3)/2 \leq r \leq n-2$.

1. *If $(i,j;k)$ is deleted from the lower triangle, then every cell (u,v), with $0 \leq u,v < k$, and $r < u+v < k$ can be filled with entry $u+v$.*
2. *If $(i,j;k)$ is deleted from the upper triangle, then every cell (u,v), with $k+1 < u,v \leq n-1$ and $k < u+v \leq r$ can be filled with entry $u+v$.*

Proof. We will prove only the first part, since the proof of the second part will be similar:

The set C, with $(i,j;k)$ deleted from the lower triangle, and represented by *, is as follows:

0	1	...	r					
1	...	r						
...	r							
r								
								r+1
								...
						r+1	*	n−3
					r+1	...	n−3	n−2

The element $r+1$ occurs in rows $r+2$ to $n-1$. Thus in column 0, there is only one cell that can be filled by $r+1$, and that is position $(r+1,0)$. Fill this. Consider now cell $(r,1)$. Element $r+1$ occurs once in each of the rows $r+1,\ldots,n-1$. Thus there is only one cell that can be

filled with $r+1$, and that is $(r,1)$. Similarly, one can show, that each of the other cells in the diagonal

$$\{(u,v;u+v) : 0 \leq u \leq r+1, 0 \leq v \leq r+1, u+v = r+1\}$$

can be filled. A similar proof can be made for each of the other diagonals given above. □

Lemma 3 *Suppose $(i,j;k)$ is deleted from C. Apart from the empty positions given in lemmas 1 and 2, no other empty position in the partial latin square can be uniquely filled.*

Proof. To help understand the proof we give below an example of a partial latin square of order 9. This partial latin square has been obtained by deleting the entry $(7,7;5)$ from the critical set given in Example 1, and then obtaining the nest of this entry, by applying Lemmas 1 and 2. We claim that no empty entry in this partial latin square can be uniquely filled.

0	1	2	3	4				8
1	2	3	4					0
2	3	4						1
3	4							2
4								3
								4
							4	5
						4		6
8	0	1	2	3	4	5	6	7

We now give the proof of the lemma. Suppose that the entry $(i,j;k=i+j)$ was deleted from the lower triangle in C. From Lemma 1 each of the rows $\gamma, i < \gamma \leq n-1$ can be uniquely filled, as can every column $\lambda, j < \lambda \leq n-1$. By lemma 2, each of the cells (u,v), with $0 \leq u,v < k$ and $r < u+v < k$ can be uniquely filled.

Of the unfilled cells, the cells $(r+2,0),(0,r+2),(i,0)$, and $(0,j)$ have the most information pertaining to them; that is, the union of the row and column containing each of these cells have more non-empty cells than any of the other cells. Thus we need only show that these cells cannot be uniquely filled.

Now row i contains each of the elements $i, i+1, \ldots, k-1, k+1, \ldots, r$, and column j the elements $j, j+1, \ldots, k-1, k+1, \ldots, r$. Thus any of the elements $0, 1, \ldots, min\{i,j\}-1, k, r+1, r+2, \ldots, n-1$ can fill cell (i,j), and so (i,j) cannot be uniquely filled. Consequently no other empty cell in row i can be uniquely filled, and no other empty cell in column j can be uniquely filled. Thus neither cell $(i,0)$ nor cell $(0,j)$ can be uniquely filled. Since cell $(i,0)$ cannot be uniquely filled, no empty cell in column 0 can be uniquely filled, and thus cell $(r+2,0)$ cannot be uniquely filled. Similarly, since cell $(0,j)$ cannot be uniquely filled, no empty cell in row 0 can be filled.

Similar arguments can be used if an entry was deleted from the upper triangle in C. □

We now summarise the above results as follows:

Theorem 3 *Let C be the critical set given in the beginning. If an entry $(i,j;k=i+j)$ is deleted from the lower triangle in C, then every column λ, $j < \lambda \leq n-1$, and every row γ, $i < \gamma \leq n-1$ can be uniquely filled, as can every cell (u,v), with $r < u+v \leq k-1$. These are diagonals in the upper triangle, going from the upper right to the lower left. No other empty cell*

can be filled uniquely. Having filled these cells, the resulting partial latin square has size

$$|\mathcal{N}(\{(i,j;k)\})| = cr - 1 + \sum_{\gamma=i+1}^{n-1}[n-(\gamma-(r+1))] + \sum_{\lambda=j+1}^{n-1}[n-(\lambda-(r+1))] + \sum_{\alpha=r+2}^{k}\alpha$$

where cr is the size of the original critical set, the first summation is the number of entries filled in the rows γ, the second summation gives the number of entries filled in the columns λ, and the last summation gives the number of entries in the diagonals that are filled.

Similarly, if an entry $(i,j;k)$ is deleted from the upper triangle in C, then

$$|\mathcal{N}(\{(i,j;k)\})| = cr - 1 + \sum_{\gamma=0}^{i-1}[n+\gamma-r-1] + \sum_{\lambda=0}^{j-1}[n+\lambda-r-1] + \sum_{\alpha=n-r-1}^{n-k-2}\alpha$$

or

$$|\mathcal{N}(\{(i,j;k)\})| = cr - 1 + \sum_{\gamma=1}^{i}[n+\gamma-r-2] + \sum_{\lambda=1}^{j}[n+\lambda-r-2] + \sum_{\alpha=n-r-1}^{n-k-2}\alpha$$

Here the first summation is the number of entries filled in the rows γ, the second summation is the number of columns filled, and the third summation is the number of diagonals that are filled.

Proof. The proof follows from the above lemmas. □

Now, the critical set has size:

$$cr = \frac{1}{2}[(r+1)(r+2) + (n-r-2)(n-r-1)]$$

Lemma 4 *The above summations may be simplified as follows:*

S1. $\sum_{\gamma=i+1}^{n-1}[n-(\gamma-(r+1))] = (n-i-1)(n+r+1) - \frac{1}{2}[n(n-1) - i(i+1)]$

S2. $\sum_{\lambda=j+1}^{n-1}[n-(\lambda-(r+1))] = (n-j-1)(n+r+1) - \frac{1}{2}[n(n-1) - j(j+1)]$

S3. $\sum_{\gamma=1}^{i}[n+\gamma-r-2] = \frac{i}{2}[2(n-r-2) + (i+1)]$

S4. $\sum_{\lambda=1}^{j}[n+\lambda-r-2] = \frac{j}{2}[2(n-r-2) + (j+1)]$

S5. $\sum_{\alpha=r+2}^{k}\alpha = \frac{1}{2}[k(k+1) - (r+1)(r+2)]$

S6. $\sum_{\alpha=n-r-1}^{n-k-2}\alpha = \frac{1}{2}[(n-k-2)(n-k-1) - (n-r-2)(n-r-1)]$

□

We note that $S1$ and $S2$ are the same function, which we will denote by $\underline{f}$. This function denotes the total number of entries in the rows or columns that are filled, when an entry is deleted from the lower triangle of C. Also, $S3$ and $S4$ represent the same function, which we denote by $\overline{f}$, which gives the total number of entries in the rows or columns that are filled, when an entry is deleted from the upper triangle of C. We relabel $S5$ by the function notation $\underline{g}$, which gives the total number of entries in the diagonals that are filled when an entry is deleted from the lower triangle of C. Similarly, we relabel $S6$ by the function $\overline{g}$, which gives the total number of entries in the diagonals that are filled when an entry is deleted from the upper triangle of C. That is:

1. $\underline{f}(r,x) = (n-x-1)(n+r+1) - \frac{1}{2}[n(n-1) - x(x+1)]$

2. $\overline{f}(r,x) = \frac{x}{2}[2(n-r-2)+(x+1)]$
3. $\underline{g}(k,r) = \frac{1}{2}[k(k+1)-(r+1)(r+2)]$
4. $\overline{g}(k,r) = \frac{1}{2}[(n-k-2)(n-k-1)-(n-r-2)(n-r-1)]$

Then,

Theorem 4 *The number of cells that can be completed after deletion of an element from the lower triangle and upper triangle, respectively, are:*

1. *If $(i,j;k)$ is deleted from the* lower *triangle in C, then*

$$|\mathcal{N}((i,j;k))| = \underline{f}(r,j) + \underline{f}(r,i) + \underline{g}(k,r) + cr - 1.$$

and

2. *if $(i,j;k)$ is deleted from the* upper *triangle in C, then*

$$|\mathcal{N}((i,j;k))| = \overline{f}(r,j) + \overline{f}(r,i) + \overline{g}(k,r) + cr - 1,$$

□

Theorem 5 *If x and y are any two triples in C, then $\mathcal{N}(\{x,y\}) = \mathcal{N}(\{x\}) \cap \mathcal{N}(\{y\})$.*

Proof. Since $\{x,y\} \supset \{x\}$ therefore $\mathcal{N}(\{x,y\}) \subseteq \mathcal{N}(\{x\})$. Similarly, $\mathcal{N}(\{x,y\}) \subseteq \mathcal{N}(\{y\})$. Thus taking intersections, we get $\mathcal{N}(\{x,y\}) \subseteq \mathcal{N}(\{x\}) \cap \mathcal{N}(\{y\})$.

We now need to show that $\mathcal{N}(\{x\}) \cap \mathcal{N}(\{y\}) \subseteq \mathcal{N}(\{x,y\})$. If $z \in \mathcal{N}(\{x\}) \cap \mathcal{N}(\{y\})$, then $z \in \mathcal{N}(\{x\})$ and $z \in \mathcal{N}(\{y\})$. That is, z can be uniquely filled after both elements x and y have been deleted from C. But then $z \in \mathcal{N}(\{x,y\})$. □

Theorem 6 *If $b_1, b_2, \ldots, b_n$ are any n distinct elements in B, then*

$$\mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_n\}) = \mathcal{N}(\{b_1, b_2, \ldots, b_n\}).$$

Proof. Trivially,

$$\mathcal{N}(\{b_1, b_2, \ldots, b_n\}) \subseteq \mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_n\}),$$

so we need to show that

$$\mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_n\}) \subseteq \mathcal{N}(\{b_1, b_2, \ldots, b_n\}).$$

Suppose that for some $k \leq n$,

$$\mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_k\}) \subseteq \mathcal{N}(\{b_1, b_2, \ldots, b_k\}).$$

We want to show that

$$\mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_{k+1}\}) \subseteq \mathcal{N}(\{b_1, b_2, \ldots, b_{k+1}\}).$$

Now

$$\begin{aligned} &\mathcal{N}(\{b_1\}) \cap \mathcal{N}(\{b_2\}) \cap \ldots \cap \mathcal{N}(\{b_k\}) \cap \mathcal{N}(\{b_{k+1}\}) \\ &\subseteq \mathcal{N}(\{b_1, b_2, \ldots, b_k\}) \cap \mathcal{N}(\{b_{k+1}\}) \end{aligned}$$

If $z \in \mathcal{N}(\{b_1, b_2, \ldots, b_k\}) \cap \mathcal{N}(\{b_{k+1}\})$ then $z \in \mathcal{N}(\{b_1, b_2, \ldots, b_k\})$ and $z \in \mathcal{N}(\{b_{k+1}\})$. That is, z can be uniquely filled after the elements $b_1, b_2, \ldots, b_k, b_{k+1}$ are deleted from C, and thus $z \in \mathcal{N}(\{b_1, b_2, \ldots, b_{k+1}\})$. From this and the above theorem the proof follows. □

Corollary 1 *Let L and C be as above.*

1. *Then for any set $B \subseteq C$,*
$$\mathcal{N}(B) = \cap\{\mathcal{N}(\{b\}) : b \in B\}.$$
and
2. *For any two sets $A, B \subseteq C$, $\mathcal{N}(A \cup B) = \mathcal{N}(A) \cap \mathcal{N}(B)$.*

Proof. We shall prove only 2. Let $A = \{a_1, \ldots, a_s\}$, and $B = \{b_1, \ldots, b_t\}$. Then

$$\mathcal{N}(A \cup B) = \mathcal{N}(\{a_1, \ldots, a_s, b_1, \ldots, b_t\})$$
$$= \mathcal{N}(\{a_1\}) \cap \ldots \cap \mathcal{N}(\{a_s\}) \cap \mathcal{N}(\{b_1\}) \cap \ldots \cap \mathcal{N}(\{b_t\})$$
$$= \mathcal{N}(A) \cap \mathcal{N}(B)$$

□

3 Latin Collections

Remark. Let A be a set of cells. A way of showing that no cell in A can be filled uniquely, would be to show that there exists a latin collection where each element of the collection has the same shape as A. We present below a couple of examples of such collections.

The partial latin square below is a critical set C with unique completion next to it:

0	1	2	3	
1	2	3		
2	3			
3				

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

Example 2 If $x = (0, 0; 0)$ then $C \setminus \{x\}$ has the following partial completion and full completions:

	1	2	3	
1	2	3		
2	3			1
3			1	2
		1	2	3

0	1	2	3	4
1	2	3	**4**	**0**
2	3	**4**	**0**	1
3	**4**	**0**	1	2
4	**0**	1	2	3

4	1	2	3	**0**
1	2	3	**0**	**4**
2	3	**0**	**4**	1
3	**0**	**4**	1	2
0	**4**	1	2	3

The partial latin square on the above left is in fact the nest of the entry $x = (0, 0; 0)$. The completions on the right are completions from $C \setminus \{x\}$. The bold entries in the two complete latin squares indicate the entries that have no unique completion ... these sets of entries in fact form latin interchanges, with each set being the disjoint mate of the other. *Note that a pair of latin interchanges form a latin collection of size 2.*

Example 3 If $x = (0, 1; 1)$ then $C \setminus \{x\}$ has the following partial completion and full completions:

0		2	3	
1	2	3		
2	3			
3				2
4			2	3

0	**1**	2	3	4
1	2	3	4	**0**
2	3	4	**0**	**1**
3	4	**0**	**1**	2
4	**0**	**1**	2	3

0	4	2	3	**1**
1	2	3	**0**	4
2	3	4	**1**	**0**
3	**0**	**1**	4	2
4	**1**	**0**	2	3

0	4	2	3	**1**
1	2	3	**0**	4
2	3	**1**	4	**0**
3	**0**	4	**1**	2
4	**1**	**0**	2	3

The set of non-empty cells in the partial latin square on the extreme left indicates the nest of the entry $x = (0, 1; 1)$. The three latin squares to the right are three completions from $C \setminus \{x\}$. These three full latin squares are necessary to show that each cell that is in bold type can be filled at least two ways. The three sets in bold make up a latin collection.

4 Influence of a set

Theorem 7 *For any $x \in C$, $x \in \mathcal{I}(\{x\})$, and for any $y \in C$, such that $x \neq y, x \notin \mathcal{I}(\{y\})$.*

Proof. By definition $\mathcal{I}(\{x\}) = L \setminus \mathcal{N}(\{x\})$. Since $\mathcal{N}(\{x\})$ cannot contain x, therefore $x \in \mathcal{I}(\{x\})$. Also, by definition, $C \setminus \{x\} \subset \mathcal{N}(\{x\})$, and therefore $y \in \mathcal{N}(\{x\})$. That is, $y \notin \mathcal{I}(\{x\})$. □

Theorem 8 *The influence-set of a set $B \subseteq C$ is the intersection of the influence-sets of its elements.* □

Proof. If $B \subseteq C$ then by definition

$$\begin{aligned} \mathcal{I}(B) &= L \setminus \cup\{\mathcal{N}(b) : b \in B\} \\ &= \cap\{L \setminus \mathcal{N}(b) : b \in B\} \\ &= \cap\{I(b) : b \in B\} \end{aligned}$$

□

Theorem 9 *For any two elements $x, y \in C$ such that $x \neq y$; $x \notin \mathcal{I}(\{x, y\})$, and $y \notin \mathcal{I}(\{x, y\})$.*

Proof. We have that $\mathcal{I}(\{x, y\}) = \mathcal{I}(\{x\}) \cap \mathcal{I}(\{y\})$. Since $x \notin \mathcal{I}(\{y\})$ and $y \notin \mathcal{I}(\{x\})$ we have the required result. □

Corollary 2 *For any set $A \subset C$, with $|A| \geq 2$, $A \cap \mathcal{I}(A) = \phi$.* □

Theorem 10 *Let L be a back circulant Latin square of order n with critical set C. If the lower (or upper) triangle in C has only one element, then there exists exactly one element having perfect influence.*

Proof. Suppose the lower triangle in C consists of only a single entry. Delete this entry. Then no empty entry can be uniquely completed. □

Notation 1 *For ease of notation, we will denote the points on the boundaries of the two triangles by special symbols. In the upper triangle, let:*

1. $\alpha = (0, 0; 0)$,

2. $\alpha_1 = (r, 0; r)$,

3. $\alpha_2 = (0, r; r)$,

4. α_{row} *be any entry in row* 0, *between* α *and* α_1, *exclusive*

5. α_{col} *be any entry in column* 0, *between* α *and* α_2, *exclusive*

6. α_{diag} *be any entry in the largest diagonal from lower left to upper right, in the upper triangle, between* α_1 *and* α_2, *exclusive.*

In the lower triangle, let:

1. $\beta = (n-1, n-1; n-2)$,

2. $\beta_1 = (n-1, r+2; r+1)$,

3. $\beta_2 = (r+2, n-1; r+1)$,

4. β_{row} *be any entry in row* $n-1$, *between* β_1 *and* β, *exclusive*

5. β_{col} *be any entry in column* $n-1$, *between* β_2 *and* β, *exclusive*

6. β_{diag} *be any entry in the largets diagonal from the lower left to upper right, in the lower triangle, between* β_1 *and* β_2, *exclusive.*

We first calulate the nest of each of the six corner entries of the two triangles in C.

Theorem 11 *Let* L *and* C *be the latin square and critical set discussed above. Then the six corner entries in the two triangles of* C, *have the following nests:*

1. $\mathcal{N}(\alpha) = \{(u, v; u+v) : 1 < u, v \leq n-1 \text{ and } 0 < u+v \leq r\} \cup C \setminus \{\alpha\}$

2. $\mathcal{N}(\beta) = \{(u, v; u+v)) : 0 \leq u, v < n-2 \text{ and } r < u+v < n-2\} \cup C \setminus \{\beta\}$.

3. $\mathcal{N}(\alpha_1) = \{(r+1, 0; r+1), \ldots, (n-1, 0; n-1); (r, 1; r+1), \ldots, (n-1, 1; 0); \ldots;$
$(2, r-1; r+1), \ldots, (n-1, r-1; r-2)\} \cup C \setminus \{\alpha_1\}$

4. $\mathcal{N}(\alpha_2) = \{(0, r+1; r+1), \ldots, (0, n-1; n-1); (1, r; r+1), \ldots, (1, n-1; 0); \ldots; (r-1, 2; r+1), \ldots, (r-1, n-1; r-2)\} \cup C \setminus \{\alpha_2\}$

5. $\mathcal{N}(\beta_1) = (0, r+3; r+3), \ldots, (n-3, r+3; r); (0, r+4; r+4), \ldots, (n-4, r+4; r); \ldots; (0, n-1; n-1), \ldots, (r+1, n-1; r)\} \cup C \setminus \{\beta_1\}$

6. $\mathcal{N}(\beta_2) = \{(r+3, 0; r+3), \ldots, (r+3, n-3; r); (r+4, 0; r+4), \ldots, (r+4, n-4; r); \ldots; (n-1, 0; n-1), \ldots, (n-1, r+1; r)\} \cup C \setminus \{\beta_2\}$.

Proof. Apply lemmas 1,2 and 3 □

Corollary 3 *Let* L *and* C *be the latin square and critical set as given above, of order* n. *Then for some choices of* $((i, j; k)$ *:*

1. $|\mathcal{N}(\alpha)| = \frac{1}{2}[(n-2)(n-1) + (r+1)(r+2)] - 1$

2. $|\mathcal{N}(\beta)| = \frac{1}{2}[(n-2)(n-1) + (n-r-2)(n-r-1)] - 1$

3. $|\mathcal{N}(\alpha_1)| = \frac{1}{2}[(n-r-2)(n+r-1)+2(r+1)^2]-1$

4. $|\mathcal{N}(\alpha_2)| = \frac{1}{2}[(n-r-2)(n+r-1)+2(r+1)^2]-1$

5. $|\mathcal{N}(\beta_1)| = (n-r-3)(n+r+1)+\frac{1}{2}[(n-r-2)(n-r-1)+2(r+2)^2-n(n-1)]-1$

6. $|\mathcal{N}(\beta_2)| = (n-r-3)(n+r+1)+\frac{1}{2}[(n-r-2)(n-r-1)+2(r+2)^2-n(n-1)]-1$

□

In the case where n is odd, we have:

Theorem 12 *Let L be a latin square of order $n \geq 9$, let $r = \frac{n-3}{2}$ for n odd, and $r = \frac{n-2}{2}$ for n even. Then the following pairs of entries have perfect influence:*

1. $\{\alpha, \beta\}$.

2. $\{\alpha_1, \beta_1\}$

3. $\{\alpha_2, \beta_2\}$

Proof.

1. If α is deleted then every diagonal below the main diagonal going from lower left to upper right, except the main diagonal and the one immediately below it, can be filled. Also, if β is deleted, then every diagonal, above the main diagonal going from lower left to upper right, except the main diagonal and the one immediately above it, can be filled. No diagonal above the main diagonal can intersect a diagonal below the main diagonal. (Indeed no two diagonals can intersect). That is, $\mathcal{N}(\alpha) \cap \mathcal{N}(\beta) = C \setminus \{\alpha, \beta\}$, and we're done. Thus the pair $\{\alpha, \beta\}$ have perfect influence.

2. If α_1 is deleted then every column $\lambda, 0 \leq \lambda \leq r-1$, can be filled. No other row, column or diagonal can be filled. If β_1 is deleted, then every column $\lambda, r+3 \leq \lambda \leq n-1$, can be filled. No other row, column or diagonal can be filled. Here again, the influences of α_1 and β_1 have no intersection outside of the critical set, so $\mathcal{N}(\alpha_1) \cap \mathcal{N}(\beta_1) = C \setminus \{\alpha_1, \beta_1\}$. That is, the pair $\{\alpha_1, \beta_1\}$ have perfect influence.

3. If α_2 is deleted then every row $\gamma, 0 \leq \gamma \leq r-1$, can be filled. No other row, column or diagonal can be filled. If β_2 is deleted, then every row, $\gamma, r+3 \leq \gamma \leq n-1$, can be filled. No other row, column or diagonal can be filled. The influences of α_2 and β_2 have no intersection outside of the critical set, and so $\mathcal{N}(\{\alpha_2, \beta_2\}) = C \setminus \{\alpha_2, \beta_2\}$. Thus the pair $\{\alpha_2, \beta_2\}$ have perfect influence.

□

Theorem 13 *Let L be a Latin square of odd order, and let $r = \frac{n-3}{2}$. Then the following sets of three entries each have perfect influence:*

1. $\{\alpha, \beta^*_{row} = (n-1, s; s-1), \beta^*_{col} = (t, n-1; t-1)\}$, where $r+2 \leq s \leq n-2$, and $3r-s+2 \leq t \leq n-2$.

2. $\{\beta, \alpha^*_{row} = (0, s; s), \alpha^*_{col} = (t, 0; t)\}$, where $1 \leq s, t \leq r$ and $s+t = r+1$

3. $\{\alpha_1, \alpha_2, \beta_{diag}\}$

4. $\{\beta_1, \beta_2, \alpha_{diag}\}$

5. $\{\alpha, \alpha_1, \beta_{row}\}$

6. $\{\alpha, \alpha_2, \beta_{col}\}$

7. $\{\beta, \beta_1, \beta_{row}\}$

8. $\{\beta, \beta_2, \alpha_{col}\}$

Proof.

1. Suppose α is deleted. Then each of the diagonals, below the main diagonal going from lower left to upper right, except the main diagonal, and the diagonal immediately below the main diagonal, can be filled. The other two entries deleted are from the lower triangle. Any diagonal in the upper triangle that is filled after the deletion of any of these entries cannot intersect with the set of elements completed after the deletion of α, outside of C, and so we need not consider any such diagonal. From the results in section 2, we need only check that row $t+1$, and column $s+1$ do not intersect outside of C. But since the smallest sum of s and t is $r+1$, and the largest is $n-2$, we obtain the required result. That is, for the given s and t values, $\mathcal{N}(\{\alpha, (n-1, s; s-1), (t, n-1; t-1)\}) = C \setminus \{\alpha, (n-1, s; s-1), (t, n-1; t-1)\}$.

2. If β is deleted then each diagonal, above the main diagonal going from lower left to upper right, except the main diagonal, and the diagonal immediately above the main diagonal, can be filled. The other two entries are deleted from the upper triangle. Similar to the proof of (1.) above, we need only show that row $t-1$ and column $s-1$ intersect inside C. But this is tantamaount to showing that $0 \leq t-1+s-1 \leq r$, and this can be easily achieved from the inequalities defining s and t above.

3. If α_1 is deleted, then each of the columns $\lambda, 0 \leq \lambda \leq r-1$ can be completed. No other row, column or diagonal can be completed. If α_2 is deleted, then each of the rows $\gamma, 0 \leq \gamma \leq r-1$ can be completed. No other row, column or diagonal can be completed. The set of entries that can be completed after the deletion of both α_1 and α_2 is precisely the intersection of the sets of entries that can be completed after the deletion of each of these elements seperately. This set is the region bounded by the diagonal above the main diagonal from lower left to upper right, (but excluding this diagonal), and column r and row r, again excluding these row and column. The entries that can be completed after deletion of β_{diag} will occur in rows below the row containing β_{diag} and in columns to the right of the column containing β_{diag}. This row and column cannot intersect the above set of filled entries discussed above, and so $\mathcal{N}(\{\alpha_1, \alpha_2, \beta_{diag}\}) = C \setminus \{\alpha_1, \alpha_2, \beta_{diag}\}$. Thus we have perfect influence.

4. The proof is similar to the proof of the above.

5. If α is deleted then all the diagonals below the main diagonal going from the lower left to the upper right, except the main diagonal and the diagonal immediately below it, can be filled. If α_1 is deleted then each of the columns to the left of the column containing α_1 can be filled. These sets of filled entries intersect in a region to the left of the lower triangle of C, and below the main diagonal. If β_{row} is deleted then any filled entries will occur in the columns to the right of column containing this entry. Thus the intersection of this set of filled entries, and the set of entries filled on deletion of α, occurs to the right of the lower triangle, and below the main diagonal. Clearly the two intersections do not themselves intersect. Thus $\mathcal{N}(\{\alpha, \alpha_1, \beta_{row}\}) = C \setminus \{\alpha, \alpha_1, \beta_{row}\}$.

6. The proof is similar to the above.

7. The proof is similar to the above.

8. The proof is similar to the above.

□

Theorem 14 *The following set of four entries has perfect influence:*

$$\{\alpha_{row}, \alpha_{col}, \beta_{row}, \beta_{col}\}$$

Proof. The set of entries that can be completed after the deletion of both the entries α_{row} and α_{col} will occur entirely above the main diagonal going from lower left to upper right. The set of entries that can be completed after the deletion of both the entries, β_{row} and β_{col}, will lie entirely below the diagonal going from lower left to upper right. Thus the two sets have an empty intersection, giving $\mathcal{N}(\{\alpha_{row}, \alpha_{col}, \beta_{row}, \beta_{col}\}) = C \setminus \{\alpha_{row}, \alpha_{col}, \beta_{row}, \beta_{col}\}$. Thus the set has perfect influence. □

Theorem 15 *The strong box $\mathcal{I}(C)$ is given by*

$$L \setminus \cup\{\mathcal{N}(\alpha), \mathcal{N}(\beta), \mathcal{N}(\alpha_1), \mathcal{N}(\alpha_2), \mathcal{N}(\beta_1), \mathcal{N}(\beta_2)\}$$

and has size

$$0 \leq \theta(C) \leq 6$$

for n even, and

$$0 \leq \theta(C) \leq 7$$

for n odd.

Proof. If α is deleted then every diagonal below the main diagonal going from lower left to upper right can be completed, except the main diagonal and the diagonal immediately below it. This is the maximum number of diagonals that can be filled on deletion of any set from C. Also, if β is deleted, then we can fill all the diagonals above the main diagonal, excluding the main diagonal, and the one immediately above it. This is the maximum number of diagonals that can be filled above the main diagonal. Similarly the deletion of the remaining entries gives the maximum number of rows, and columns that can be filled. Thus the cells that are not in the union of the nests of these elements must form the influence of C. That is, $\mathcal{I}(C) = L \setminus \cup\{\mathcal{N}(\alpha), \mathcal{N}(\beta), \mathcal{N}(\alpha_1), \mathcal{N}(\alpha_2), \mathcal{N}(\beta_1), \mathcal{N}(\beta_2)\}$

If $r = n - 2$ then C consists of only the upper triangle. It is easy to check that the union of the nests of the entries cover the whole latin square. Thus there is no influence when all these entries are deleted. That is, $\mathcal{I}(C) = \phi$, so $\theta(C) = 0$.

Let n be even, and $r = \frac{n-2}{2}$. Then the union of the nests of the above entries cover all the columns except columns r to $r+2$, all rows except rows r to $r+2$, all the diagonals going from lower left to upper right, except those diagonals beginning from the cells $(n-2, 0), (n-1, 0), (n-1, 1)$. This union covers all entries, except the entries $(r, r), (r, r+1), (r, r+2); (r+1, r), (r+1, r+1); (r+2, r+2)$. Thus $\mathcal{I}(C) = (r, r), (r, r+1), (r, r+2); (r+1, r), (r+1, r+1); (r+2, r+2)$, and $\theta(C) = 6$.

Let n be odd, and $r = \frac{n-3}{2}$. Then the union of the nests of these entries cover all cells,

except $(r,r+1),(r,r+2);(r+1,r),(r+1,r+1),(r+1,r+2);(r+2,r),(r+2,r+1)$. Thus, $\mathcal{I}(C) = r,r+1),(r,r+2);(r+1,r),(r+1,r+1),(r+1,r+2);(r+2,r),(r+2,r+1)$, and $\theta(C) = 7$.

□

5 A hierachy of influence

Clearly,

Theorem 16 *For any three elements $x,y,z \in C$, $x \longrightarrow y$ and $y \longrightarrow z \Longrightarrow x \longrightarrow z$.* □

Example 4 Consider the critical set for the 7×7 back circulant latin square:

0	1	2				
1	2					
2						
						3
					3	4
				3	4	5

Let $\alpha = (0,0;0), \alpha_1 = (0,2;2), \alpha_2 = (2,0;2), \alpha_{row} = (0,1;1), \alpha_{col} = (1,0;1), \alpha_{diag} = (1,1;2), \beta = (6,6;5), \beta_1 = (6,4;3), \beta_2 = (4,6;3), \beta_{row} = (6,5;4), \beta_{col} = (5,6;4), \beta_{diag} = (5,5;3)$. The nests of these entries are as follows:

	1	2				
1	2					
2						1
					1	2
				1	2	3
			1	2	3	4
		1	2	3	4	5

Nest of α

0	1					
1	2					
2	3					
3	4					
4	5					3
5	6				3	4
6	0			3	4	5

Nest of α_1

0	1	2	3	4	5	6
1	2	3	4	5	6	0
						3
					3	4
				3	4	5

Nest of α_2

0		2				
1	2					
2						
3						2
4					2	3
5				2	3	4
6			2	3	4	5

Nest of α_{row}

0	1	2	3	4	5	6
	2					
2						
						2
					2	3
				2	3	4
			2	3	4	5

Nest of α_{col}

0	1	2	3	4	5	6
1						
2						
3						
4						3
5					3	4
6				3	4	5

Nest of α_{diag}

0	1	2	3	4		
1	2	3	4			
2	3	4				
3	4					
4						3
					3	4
				3	4	

Nest of β

0	1	2			5	6
1	2				6	0
2					0	1
					1	2
					2	3
					3	4
					4	5

Nest of β_1

0	1	2				
1	2					
2						
5	6	0	1	2	3	4
6	0	1	2	3	4	5

Nest of β_2

0	1	2	3			6
1	2	3				0
2	3					1
3						2
						3
					3	4
				3		5

Nest of β_{row}

0	1	2	3			
1	2	3				
2	3					
3						
						3
					3	
6	0	1	2	3	4	5

Nest of β_{col}

0	1	2				6
1	2					0
2						1
						2
						3
						4
6	0	1	2	3	4	5

Nest of β_{diag}

From inspection of the nests, we find that the following sets have perfect influence:

1. $\{\alpha, \beta\}$
2. $\{\alpha, \alpha_1\}, \{\alpha, \alpha_2\}, \{\alpha, \alpha_{diag}\}, \{\alpha_1, \alpha_2\}, \{\alpha_1, \alpha_{col}\}, \{\alpha_2, \alpha_{row}\}$
3. $\{\beta, \beta_1\}, \{\beta, \beta_2\}, \{\beta, \beta_{diag}\}, \{\beta_1, \beta_2\}, \{\beta_1, \beta_{col}, \{\beta_2, \beta_{row}\}$
4. $\{\alpha_1, \beta_1\}, \{\alpha_2, \beta_2\}$
5. $\{\alpha, \beta_{row}, \beta_{col}\}, \{\beta, \alpha_{row}, \alpha_{col}\}$
6. $\{\alpha_{row}, \alpha_{col}, \beta_{row}, \beta_{col}\}$

From these perfect influence sets we have that $\alpha \rightsquigarrow \alpha_{row}, \alpha \rightsquigarrow \alpha_{col}$, and $\beta \rightsquigarrow \beta_{row}, \beta \rightsquigarrow \beta_{col}$. That is, α is more influential than α_{row} and α_{col}, etc. In terms of perfect influence, it means, for example, that given any set A of non-perfect influence, if $\alpha_{row}A$ has perfect influence, then αA will also have perfect influence. Similarly, if $\{\alpha_{row}, \alpha_{col}\} \cup A$ has perfect influence, then αA will also have perfect influence.

The table below is obtained by replacing each entry in C with its influence:

29	30	29				
30	30					
29						
						29
					30	30
				29	30	29

That is,

$$\theta(\alpha) = \theta(\beta) = \theta(\alpha_1) = \theta(\alpha_2) = \theta(\beta_1) = \theta(\beta_2) = 29,$$

$$\theta(\alpha_{row}) = \theta(\alpha_{col}) = \theta(\alpha_{diag}) = \theta(\beta_{row}) = \theta(\beta_{col}) = \theta(\beta_{diag}) = 30.$$

So

$$[\alpha] = \{\alpha, \beta, \alpha_1, \alpha_2, \beta_1, \beta_2\} \text{ and } [\alpha_{row}] = \{\alpha_{row}, \alpha_{col}, \beta_{row}, \beta_{col}\}.$$

That is, the index of C is 2.

A secret sharing scheme is a method of dividing a secret S among a set $\mathcal{P}$ of participants in such a way that only authorised subsets of $\mathcal{P}$ can reconstruct the secret by pooling their information. A secret sharing scheme based on a critical set of a latin square would have each triple associated with the critical set distributed as shares. If the size of the critical set is t then this is a t-out-of-t scheme. (See for example [1])

In general the critical sets we have looked at are unions of two triangles of triples, one in the upper left hand corner, denoted UL, and the other in the lower right hand corner, denoted RL. In such a case the scheme is compartmentalised, as elements of both compartments are needed to complete the latin square.

We have seen that some triples have more influence than others. For example in the above diagram the triple α is more influential than β_1 and β_2. Thus the scheme is not only compartmentalised, but hierachical as well.

Supposing that $x \longrightarrow y$. How many finite sequences of the form $x \rightsquigarrow x_1 \rightsquigarrow \ldots \rightsquigarrow x_n \rightsquigarrow y$ are there? What is the length (ie the number of entries in the chain) of the longest such sequence? How does this length relate to the index of C, if at all? These and similar questions seem worthy of further investigation.

References

[1] J.Cooper, D.Donovan and J.Seberry. *Secret sharing schemes arising from Latin squares*, Bulletin of the Institute of Combinatorics and its Applications, September, (1994), 33-43.

[2] D.Curran and G.H.J.Van Rees. *Critical sets in Latin squares,* in Proc. Eighth Manitoba Conference on Numer. Math. and Computing, (1978), 165-168.

[3] D.Donovan and Joan Cooper, *Critical sets in back circulant latin squares*, Aequationes Mathematicae 52 (1996) 157-179.

[4] J.Nelder. *Critical sets in Latin squares*, CSIRO Div. of Math. and Stats, Newsletter, 38, (1977).